SVEUČILIŠTE U ZAGREBU

FILOZOFSKI FAKULTET

ODSJEK ZA INFORMACIJSKE I KOMUNIKACIJSKE ZNANOSTI

Ak. god. 2017./18.

Anamarija Torić

Privatnost na mreži, moguće zlouporabe podataka i načini zaštite

završni rad

mentor Sonja Špiranec

Zagreb, 2018.

Sažetak

Ovaj rad bavi se problematikom sigurnosti i privatnosti na mreži, te kroz analizu mogućih zlouporaba podataka nudi pregled opasnosti koje vrebaju na Internetu. Osobni podaci definiraju svakog pojedinca kao jedinstvenu individuu, te je bitno zaštititi se od mogućih povreda privatnosti. Postoje brojne organizacije koje se već godinama bore sa suzbijanjem računalnog kriminaliteta, te se kroz njihovo djelovanje mogu otkriti brojne korisne informacije o načinima zaštite. Nedavni incident vezan uz međunarodnu korporaciju Facebook osvijestio je ljude o tome koliko je zapravo lako biti žrtvom zlouporabe podataka, ali ih je isto tako potaknuo na djelovanje.

Ključne riječi

Internet Privatnost Sigurnost Zlouporaba podataka Računalni kriminalitet

Internet privacy, data misuse and protection

Abstract

This paper deals with the issue of security and privacy online, providing the insight into the dangers lurking on the Internet through the analysis of possible data misuse. Personal data is something that defines a person as a unique individual, so it's important to protect ourselves from possible privacy violations. There are many organizations that have been dealing with computer crime for years, and they can provide us with useful information on how to protect ourselves. A recent incident concerning Facebook has been a wake-up call for many, showing how easy it is to be a victim of data misuse, but has also encouraged them to take action.

Key words

Internet Privacy Safety Data misuse Computer crime

Sadržaj

Uvod

Svijet u kojem danas živimo svijet je tehnologije. Društvene mreže drže monopol nad svim ostalim oblicima ljudske interakcije. Služe nam kao oblik dodira s vanjskim svijetom i za predstavljanje slike o sebi u javnosti. Nije nam problem dijeliti određene osobne podatke, ali možda bismo trebali bolje promisliti o tome što se događa s podacima koje ne dijelimo ni sa kime. Svi mi cijenimo svoju privatnost, ali nismo uvijek svjesni trenutaka kada je ona ugrožena. Nedavni skandal vezan uz najpoznatiju društvenu mrežu, Facebook[1], osvijestio je mnoge o opasnostima koje se skrivaju na Internetu, i društvene mreže su bile prisiljene promijeniti svoju politiku u vezi s privatnošću podataka.[2] No, ne možemo sa sigurnošću znati je li se išta promijenilo. Uvjeti privatnosti su nešto na što korisnici pristanu prilikom korištenja svake internetske stranice, ali većina ne posvećuje tome previše pažnje. Moguće je čak i da korisnici nesvjesno pristaju na nešto što bi smatrali povredom vlastite privatnosti.

Još jedna od karakteristika Interneta, većini ljudi veoma korisna, maksimalna je efikasnost pretraživanja. Tražilice danas su brze i precizne, te su postale sastavni dio svakodnevice, posebice mlađim generacijama. Ustvari, toliko su neizbježne, da smo spremni žrtvovati vlastitu privatnost, svjesno ili nesvjesno. Što god radili na Internetu, iza sebe ostavljamo trag podataka, na temelju čega većina tražilica funkcionira. Oglašavanje se tvori na tom principu, pogotovo ako se među većim korporacijama odvija razmjena i prodaja osobnih podataka korisnika iz jedne baze podataka u drugu.[3]

Postoji još bezbroj primjera jer je Internet, prije svega, beskonačna mreža podataka. U današnjoj civilizaciji ne postoji opcija jednostavno se odreći korištenja Interneta kako bi se zaštitili od mogućih povreda privatnosti jer je, htjeli mi to ili ne, postao neophodan dio naših života. Jedino što je u našoj moći je otkriti koliko su korisnici svjesni mogućih zlouporaba njihovih podataka, te povećati tu svijest. Naposljetku, i jedna od najvećih korporacija kao što je

[1] Kleinman, Zoe. Cambridge Analytica: The story so far. 21.3.2018. URL: https://www.bbc.com/news/technology-43465968 (23.8.2018.)
[2] Tiku, Nitasha. Why Your Inbox Is Crammed Full of Privacy Policies. 24.5.2018. URL: https://www.wired.com/story/how-a-new-era-of-privacy-took-over-your-email-inbox/ (23.8.2018.)
[3] Miller, Michael. Apsolutna zaštita PC-ja i privatnosti. Čačak : Kompjuter biblioteka, 2003.

Facebook bila je prisiljena poduzeti određene mjere i time napraviti presedan ostalima nakon što se u javnosti pročulo što se sve događalo s našim osobnim podacima.

Ovaj rad bavi se mogućim povredama privatnosti na mreži, te načinima na koje se s njima nosilo kroz vrijeme. Cilj je povećati svijest o zlouporabi podataka, pružiti pregled najčešćih i najopasnijih povreda privatnosti, te kroz radrazličitih organizacija, kao i kroz inicijative i istraživanja koja su se bavila tim problemom, proširiti znanje i sigurnost na mreži.

1 Pojmovi privatnosti i osobnih podataka

Dva ključna pojma vezana uz temu zlouporabe podataka su sam pojam osobnih podataka, odnosno podataka koji se pripisuju određenom pojedincu, te pojam privatnosti, ili prava svakog čovjeka na vlastitu privatnost. Prema *Zakonu o zaštiti osobnih podataka*, osobni podatak definira se kao „svaka informacija koja se odnosi na identificiranu fizičku osobu ili fizičku osobu koja se može identificirati; osoba koja se može identificirati je osoba čiji se identitet može utvrditi izravno ili neizravno, posebno na osnovi identifikacijskog broja ili jednog ili više obilježja specifičnih za njezin fizički, psihološki, mentalni, gospodarski, kulturni ili socijalni identitet.“[4]

Prema tome, kao osobni podatak može se definirati širok spektar različitih podataka koji mogu izravno, ali i neizravno dovesti do otkrivanja identiteta određenog pojedinca. Svaka zlouporaba osobnih podataka je udar na privatnost osobe, s obzirom na to da joj se može otkriti identitet. Privatnost je nešto što se često spominje, kao i fraza „pravo na privatnost“, koje se smatra jednim od elementarnih prava svakoga čovjeka. „Privatnost je jedna od nosivih vrednota zapadne pravne kulture. Zasnovana je, s jedne strane, na uvjerenju da svako ljudsko biće ima vrijednost po sebi, a s druge na iskonskoj čovjekovoj potrebi za postojanjem određenog zaštićenog prostora iz kojega bi svatko drugi bio isključen psihološki i materijalno.“[5]

U svijetu tehnologije privatnost je poprimila različite oblike. Internet može pružiti okrilje anonimnosti, ali isto tako i ugroziti fundamentalno pravo svakog čovjeka na privatnost distribuiranjem njegovih osobnih podataka bez njegovog znanja, a i odobrenja. Ustvari, utjecaj tehnologije toliko je očigledan da se jedna vrsta privatnosti, komunikacijska privatnost, počela nazivati e-privatnošću[6], s obzirom na to da se velik dio komunikacije danas odvija na mreži. Neizbježno je zaključiti da je u svijetu tehnologije protok informacija dosegao do sada neviđene razmjere. Puno je lakše doći do informacija, a količina informacija koja kruži po Internetu je jednostavno nezamisliva. Nitko ne zna što se sve nalazi u beskrajnim prostranstvima Interneta,

[4] Zakon o zaštiti osobnih podataka. Zagreb : Narodne novine br. 103/2003.
[5] Boban, Marija. Sigurnost i zaštita osobnih podataka - pravni i kulturološki aspekti : doktorska disertacija. Zagreb : Filozofski fakultet u Zagrebu : Odsjek za informacijske znanosti, 2012. Str. 11.
[6] Boban, Sigurnost i zaštita osobnih podataka, n. dj.

pa se sve češće javljaju strahovi vezani uz očuvanje čovjekove privatnosti u novom tehnološkom dobu.

2 Sigurnost informacija na mreži

Danas je važnost informacija toliko velika da bismo je mogli prozvati valutom suvremenog svijeta. Informacijama se može trgovati, „a u informacijskoj ekonomiji stavlja se naglasak na informaciju kao poslovni resurs – ravnopravan sa svim ostalim resursima tvrtke.“[7]Dakle, informacija se može smatrati čovjekovom imovinom, te sukladno tome, kao što svaki čovjek ima u sebi nagon da zaštiti svoju imovinu, tako ima u sebi i nagon da zaštiti informacije koje posjeduje, odnosno svoje osobne podatke. No, do odluke za djelovanjem dođe samo kada je pojedinac svjestan da bi sigurnost njegovih podataka mogla biti ugrožena, što nije uvijek slučaj.

Kod samog pristupa mreži, ulazimo u beskonačan virtualan prostor, tzv. kibernetski prostor (*eng. cyberspace)* koji nam omogućuje povezivanje s cijelim svijetom. Na taj prostor se ne primijenjuju geografske teritorijalne granice, te ga je samim time teže regulirati.[8] Nismo ni svjesni koliko informacija i podataka kruži po mreži svakoga dana. Nemoguće je otkriti sve što se nalazi na Internetu, ali ako nam zatreba neki podatak, znamo da ćemo ga lako pronaći. Ali zato također postoji šansa i da netko ima pristup našim podacima.

Internet se temelji na razmjeni informacija, koja se odvija na dvije razine. Postoji vidljiva razmjena informacija koja se odvija na samoj površini Interneta, kada korisnici međusobno i javno dijele informacije jedni s drugima. Ali isto tako postoji i skrivena razmjena informacija, kada jedna strana nije svjesna toga da su njeni podaci završili u nečijim rukama. Osjećaj sigurnosti daju nam brojne mjere zaštite koje poduzimamo, poput lozinki na različitim društvenim mrežama koje upotrebljavamo. No, iako nas to može zaštititi od toga da netko drugi pristupi našem korisničkom računu, postoji još toliko podataka koje sasvim nesvjesno ostavljamo iza sebe, bez pomisli da bi ih netko drugi mogao iskoristiti u svoju korist. Digitalni otisak (*eng. digital footprint*) je trag koji ostavljamo iza sebe kad god nešto radimo na mreži. Isto kao i otisak prsta, jedinstven je i razlikuje se od osobe do osobe, pa nas se i pomoću njega može identificirati.

[7] Boban, Sigurnost i zaštita osobnih podataka, n. dj. Str. 52.
[8] Johnson, David R.; Post, David.Law and Borders – The Rise of Law in Cyberspace. // First Monday. 1, 1(1996)

Došlo je i do govora o digitalnom životu nakon smrti (*eng. digital afterlife)*, s obzirom na to da je trag koji ostavljamo iza sebe na mreži neizbrisiv.[9]Na sve to treba obratiti pozornost kada uzimamo u obzir načine na koje netko može doći do naših osobnih podataka.

3 Računalni kriminalitet

Što se tiče samog računalnog kriminaliteta i zlouporaba koje se uz njega vežu, one se prema M. Boban mogu podijeliti u tri grupe: zlouporaba na računalu, zlouporaba uz pomoć računala i zlouporaba učinjena računalom.[10] U slučaju zlouporaba na računalu, računalo je objekt napada, odnosno na njemu se nalaze informacije do kojih se želi doći. U slučaju zlouporaba uz pomoć računala, te onih učinjenih računalom, računalo je sredstvo napada, odnosno računalo se koristi kao alat za počinjenje zlouporabe podataka.

Od brojnih mogućih kaznenih djela, M. Boban navodi najčešća, a to su: neovlašteni pristup računalnom sustavu, računalna špijunaža, računalna sabotaža, računalna prijevara, računalno krivotvorenje, softversko piratstvo, štetni i nezakoniti sadržaji i krađa identiteta.[11]

Neovlašteni pristup računalnom sustavu može se postići na dva načina. Onaj jednostavniji bio bi da neovlašteni korisnik fizički pristupi računalu ovlaštenog korisnika radi nepažnje ovlaštenog korisnika ili krađe računala. Ali, isto tako, do neovlaštenog pristupa može doći i bez fizičkog pristupa računalu. Naime, s pojavom Interneta, pojavili su se i tzv. hakeri, koji se definiraju kao ljudi koji su „obuzeti programiranjem i kompjutorskom tehnologijom“, ali i kao ljudi koji „potajno i neovlašteno upadaju u tuđa računala i mreže, provjeravajući ili mijenjajući programe i podatke pohranjene u njima.“[12] Na meti hakera najčešće se nalaze vladine organizacije ili poznate međunarodne korporacije. Jedan od najpoznatijih hakera, o kojem je snimljen i film, je Julian Assange, osnivač međunarodne neprofitne organizacije WikiLeaks koja je objavljivala razne povjerljive podatke i informacije iz anonimnih izvora.[13]

[9]Wright, Nicola. Death and the Internet: The implications of the digital afterlife. // First Monday. 19, 6(2014)
[10] Boban, Sigurnost i zaštita osobnih podataka, n. dj. Str. 71.
[11] Ibid.
[12] Haker. // Hrvatski jezični portal (2018), URL: http://hjp.znanje.hr/index.php?show=search_by_id&id=fV5iWRE%3D&keyword=haker (23.8.2018.)
[13] Julian Assange: Campaigner or attention-seeker? 30.7.2018. URL: https://www.bbc.com/news/world-11047811 (23.8.2018.)

Prema tome, djelovanje WikiLeaksa moglo bi se smatrati iračunalnom špijunažom, koja „obuhvaća sve manipulacije kojima je osnovni cilj neovlašteno pribavljanje tajnih podataka i informacija koje se nalaze u računalnim sistemima ili u prijenosu putem komunikacijskih kanala.“[14] Računalna špijunaža ujedno i spada pod neovlaštene pristupe računalnom sustavu, samo što je u njenom slučaju specificiran cilj upada. Radi se, naime, o trgovanju podacima, te se na meti počinitelja većinom nalaze povjerljive informacije čijom prodajom ili objavljivanjem mogu ostvariti neku novčanu dobit, ili određenoj organizaciji ili korporaciji uskratiti novčanu dobit. Česti su slučajevi sabotiranja konkurencije otkrivanjem određenih službenih podataka, radi čega se pojavio i pojam „informacijskog ratovanja“[15]. Rusija je bila suočena s optužbama za informacijsko ratovanje i navodno uplitanje u američke predsjedničke izbore pomoću hakiranja elektroničkih pošti i društvenih mreža demokratskih političara, a nakon što se vijest o tome pročula, i europske zemlje su počele strahovati da bi se i one mogle naći na meti Rusije.[16]

Danas je moć informacija toliko velika, s obzirom na to da mogu pokriti velike udaljenosti u samo nekoliko trenutaka, da je jedna informacija o određenoj utjecajnoj osobi ili korporaciji dovoljna da im se život promijeni do temelja. Brojni su slučajevi u svijetu slavnih osoba kada ih je samo jedna neutemeljena optužba obilježila za cijeli život. Više nije ni toliko bitno je li informacija istinita ili ne, čim se nađe na Internetu i ljudi je počnu uočavati, šteta je već učinjena. Na Internetu je moguće razotkriti nekoga, a u isto vrijeme ostati pod krinkom anonimnosti. Zato se i pojavio pojam „tamnih brojki“ kojima se „u kriminologiji označava broj realiziranih kaznenih djela za koje se ne zna zato što nisu otkrivena i zato što je počinitelj nepoznat.“[17]Dakle, osim što je moguće da se nikada neće otkriti tko je počinitelj, isto tako je moguće da će i samo kazneno djelo ostati neotkriveno, te žrtva ni neće biti svjesna da je bila žrtva osim, naravno, ako njeni osobni podaci ne završe negdje na mreži.

Uz računalnu špijunažu, kojoj je cilj biti neprimjetna, postoji i računalna sabotaža, koja ostavlja vidljive posljedice iza sebe. Ona „obuhvaća neovlaštene aktivnosti počinjene s namjerom da se onemogući nesmetan rad ili spriječi korištenje računalnog sustava, odnosno

[14] Boban, Sigurnost i zaštita osobnih podataka, n. dj. Str. 72.
[15] Boban, Sigurnost i zaštita osobnih podataka, n. dj. Str. 90.
[16] Branford, Becky. Information warfare: Is Russia really interfering in European states? 31.3.2017. URL: https://www.bbc.com/news/world-europe-39401637 (24.8.2018.)
[17] Boban, Sigurnost i zaštita osobnih podataka, n. dj. Str. 73.

njegovih resursa.“[18]Dakle, ovdje nije riječ o krađi informacija s računala, nego o onemogućavanju samog korištenja računala, do neke mjere ili u potpunosti.

Računalna prijevara „obuhvaća razne vrste manipulacija na podacima, najčešće s namjerom da sebi i drugima nezakonito pribavi imovinsku ili neku drugu korist.“[19]Ovakav način računalnog kriminaliteta postao je češći otkad je Internet preuzeo na sebe brojne funkcije, kao što je npr. internetsko bankarstvo. Novac općenito postoji pretežito u virtualnom obliku,čime su se olakšale brojne krađe i pronevjere novca. Uz računalne prijevare usko se veže i računalno krivotvorenje, koje se odnosi na krivotvorenje postojećih dokumenata, kao i na stvaranje novih dokumenata, ali i na krivotvorenje novca.

Softversko piratstvo je nešto s čime je većina ljudi upoznata, ali ne zato što su bili žrtve, nego zato što su i sami to počinili. Na Internetu je moguće besplatno i lako preuzeti brojne računalne programe, što je oduvijek predstavljalo problem za reguliranje zaštite autorskih prava.

Kategorija štetnih i nezakonitih sadržaja razlikuje se od dosadašnjih kategorija po tome što se „zaštita proširuje sa zaštite digitalnih podataka i informacija na zaštitu od informacija.“[20]Pojava Interneta omogućila je lakše distribuiranje ovakvih sadržaja, a i teže ih je otkriti s obzirom na to da se pristup nekom sadržaju na mreži može omogućiti samo određenim korisnicima.

Krađa identiteta najosobniji je mogući način računalnog kriminaliteta, te se „definira kao oblik kriminalne radnje lažnog predstavljanja radi stjecanja materijalne ili druge koristi i predstavlja direktnu povredu privatnosti građana i Zakona o zaštiti osobnih podataka.“[21] Prema M. Boban, postoje tri osnovna tipa krađe identiteta: spoofing, phishing i skimming.[22]

Kod spoofinga, do prijevare dođe tako da počinitelj korisniku pošalje neku vrstu lažnog sadržaja, koji je naizgled identičan kao i model prema kojem je generiran. Prema tome, kod korisnika se ne pojavi nikakva sumnja, te on pristupi lažnom sadržaju i time njegovi osobni

[18] Boban, Sigurnost i zaštita osobnih podataka, n. dj. Str. 74.
[19] Boban, Sigurnost i zaštita osobnih podataka, n. dj. Str. 74.
[20] Boban, Sigurnost i zaštita osobnih podataka, n. dj. Str. 76.
[21] Boban, Sigurnost i zaštita osobnih podataka, n. dj. Str. 77.
[22] Ibid.

podaci završe u pogrešnim rukama. Jedna od najčešćih metoda spoofinga je IP spoofing[23] kada počinitelj stvara lažne adrese koje izgledaju kao stvarne i sigurne adrese. Za razliku od normalne interakcije, gdje se razmjena informacija odvija između korisnika i servera, u ovom slučaju korisnik se služi lažnom adresom koju je dobio od počinitelja, pa tako sve informacije umjesto na server, odlaze direktno do počinitelja.

Pojam phishing se odnosi na namamljivanje korisnika da im preko elektroničke pošte pošalju svoje osobne podatke kako bi riješili neki nepostojeći problem na svom korisničkom računu, ili kao kod spoofinga, kreiranje lažne stranice identične originalnoj gdje se također navodi korisnika da pruži svoje osobne podatke. Osim preko elektroničke pošte, phishing je moguć i na društvenim mrežama. Podaci do kojih počinitelji žele doći često su broj kreditne kartice ili PIN korisnika, kako bi im omogućili pristup korisnikovom bankovnom računu.[24] Prema tome, do ovakve krađe osobnih podataka najčešće dođe iz financijskih razloga.

I posljednji način, skimming, funkcionira tako da se u bankomat ugradi uređaj koji kopira podatke s kartice i kamera koja snima korisnika kako upisuje PIN.[25] Dakle, u slučajevima krađe identiteta, motivi su većinom novčanog tipa. Ono što se preporuča korisnicima je maksimalan oprez pri davanju bilo kakvih osobnih podataka.

3.1. CSI

U Sjedinjenim Američkim Državama od 1996. do 2011. Institut za istraživanje računalnog kriminaliteta (*engl. Computer Security Institute – CSI*) je objavljivao godišnja izvješća o računalnom kriminalitetu i sigurnosti (*engl. Computer Crime and Security Survey)*. Petnaesto izvješće, ujedno i posljednje, objavljeno je 2011. godine i analizira period od sredine 2009. do sredine 2010. godine. Korisnici su se izjasnili o najčešćim vrstama računalnog kriminaliteta s kojima su se susretali na mreži. (Slika 1.)

[23] Claessens, Joris; Preneel, Bart; Vandewalle, Joos. A Tangled World Wide Web of Security Issues. // First Monday. 7, 3(2002)
[24] Abad, Christopher. The economy of phishing: A survey of the operations of the phishing market. // First Monday. 10, 9(2005)
[25] Boban, Sigurnost i zaštita osobnih podataka, n. dj. Str. 77-78.

Type of Attack	2005	2006	2007	2008	2009	2010
Malware infection	74%	65%	52%	50%	64%	67%
Bots / zombies within the organization	added in 2007		21%	20%	23%	29%
Being fraudulently represented as sender of phishing messages	added in 2007		26%	31%	34%	39%
Password sniffing	added in 2007		10%	9%	17%	12%
Financial fraud	7%	9%	12%	12%	20%	9%
Denial of service	32%	25%	25%	21%	29%	17%
Extortion or blackmail associated with threat of attack or release of stolen data	option added in 2009				3%	1%
Web site defacement	5%	6%	10%	6%	14%	7%
Other exploit of public-facing Web site	option altered in 2009				6%	7%
Exploit of wireless network	16%	14%	17%	14%	8%	7%
Exploit of DNS server	added in 2007		6%	8%	7%	2%
Exploit of client Web browser	option added in 2009				11%	10%
Exploit of user's social network profile	option added in 2009				7%	5%
Instant messaging abuse	added in 2007		25%	21%	8%	5%
Insider abuse of Internet access or e-mail (i.e. pornography, pirated software, etc.)	48%	42%	59%	44%	30%	25%
Unauthorized access or privilege escalation by insider	option altered in 2009				15%	13%
System penetration by outsider	option altered in 2009				14%	11%
Laptop or mobile hardware theft or loss	48%	47%	50%	42%	42%	34%
Theft of or unauthorized access to PII or PHI due to mobile device theft/loss	option added in 2008			8%	6%	5%
Theft of or unauthorized access to intellectual property due to mobile device theft/loss	option added in 2008			4%	6%	5%
Theft of or unauthorized access to PII or PHI due to all other causes	option added in 2008			8%	10%	11%
Theft of or unauthorized access to intellectual property due to all other causes	option added in 2008			5%	8%	5%

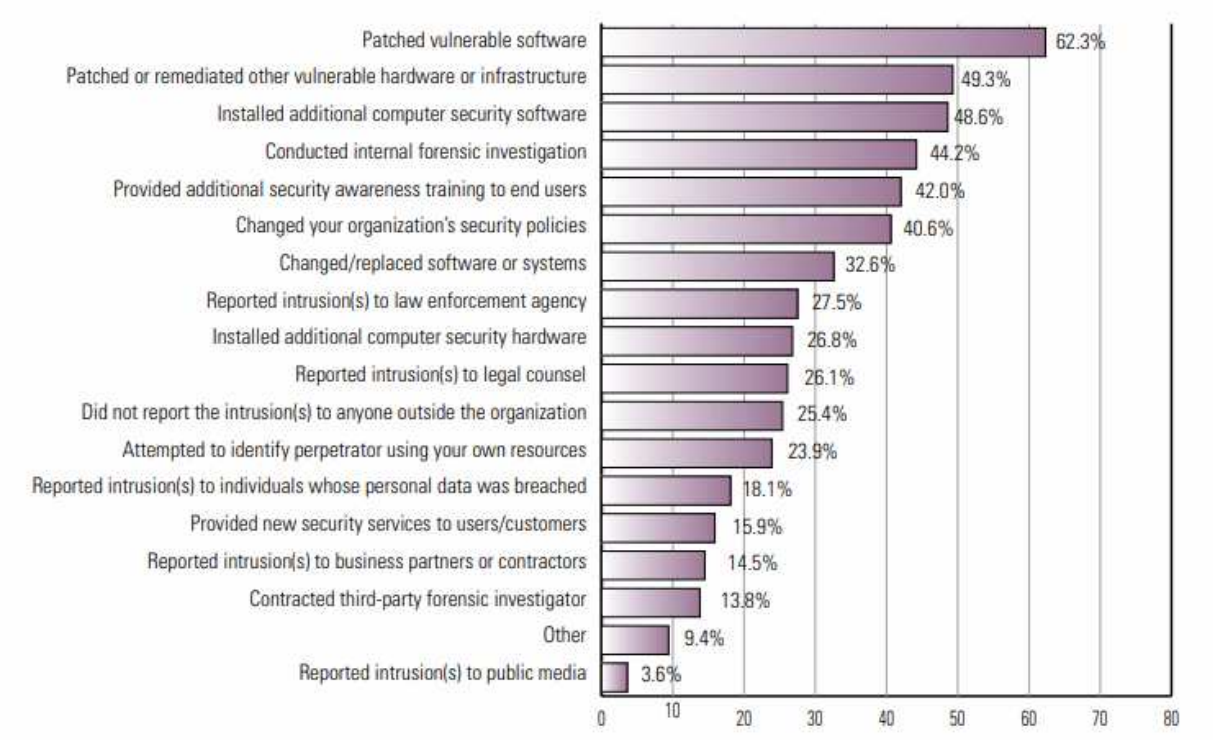
Slika 1. Računalni kriminalitet prema vrstama napada na sustav u razdoblju od 2005. do 2010. godine.[26]

Kao što je vidljivo, s vremenom su se uz razvoj Interneta počele pojavljivati i nove vrste napada i ugrožavanja sigurnosti korisnika na mreži. Od svih vrsta napada, i dalje su najzastupljeniji tzv. računalni virusi, ali već tad su postojale i razne vrste zlouporabe osobnih podataka. Iako u ovom istraživanju najmanje zastupljena, 2009. je dodana stavka koja se veže uz krađu osobnih podataka. Navode se i zlouporabe vezane uz internetski preglednik, kao i

[26]Computer Security Institute. 2010/2011 Computer Crime and Security Survey, 2011.Dostupnona: https://cours.etsmtl.ca/gti619/documents/divers/CSIsurvey2010.pdf

korisnički profil na određenoj društvenoj mreži, što su također stavke dodane 2009. godine. Krađa, kao i neovlašten pristup intelektualnoj imovini (u što ponajprije spadaju osobni podaci), aktualna je od 2008. godine. Ovdje se kao razlozi neovlaštenog pristupa spominju krađa ili gubitak mobilnog uređaja, ali postoji i stavka koja se odnosi općenito na sve ostale razloge, a zastupljena je jednako koliko i prva stavka, ako ne i više. Dakle, ovo izvješće je bilo na tragu brojnih problema vezanih uz sigurnost osobnih podataka s kojima se susrećemo danas, ali je, nažalost, 2011. godine CSI prestao postojati, pa su se i godišnja izvješća prestala provoditi.

Osim analiza mogućih vrsta napada, ova istraživanja bavila su se i reakcijama korisnika i radnjama koje su poduzimali nakon što bi iskusili napad. (Slika 2.)



Slika 2. Podaci o postupcima korisnika nakon suočavanja s računalnim kriminalom u 2010. godini[27].

S obzirom na to da je većina problema bila vezana uz računalne viruse, najviše mjera zaštite odnosi se na korištenje raznih anti-virusnih programa. Neki su se odlučili obratiti

[27]Computer Security Institute. 2010/2011 Computer Crime and Security Survey, 2011.Dostupnona: https://cours.etsmtl.ca/gti619/documents/divers/CSIsurvey2010.pdf

policijskim službenicima, pravnim savjetnicima, a nekolicina se čak obratila i medijima, što je možda i najbolja odluka s obzirom na to da su mediji danas neizmjerno utjecajni. Naravno, bilo je i onih koji su odlučili sve zadržati za sebe, ili pokušati samoinicijativno pronaći krivca, ili pak unajmiti privatnog istražitelja. U svakom slučaju, bitno je uočiti da je velika većina korisnika, nakon što su bili suočeni s nekom vrstom računalnog kriminaliteta, odlučila poduzeti nešto u vezi toga.

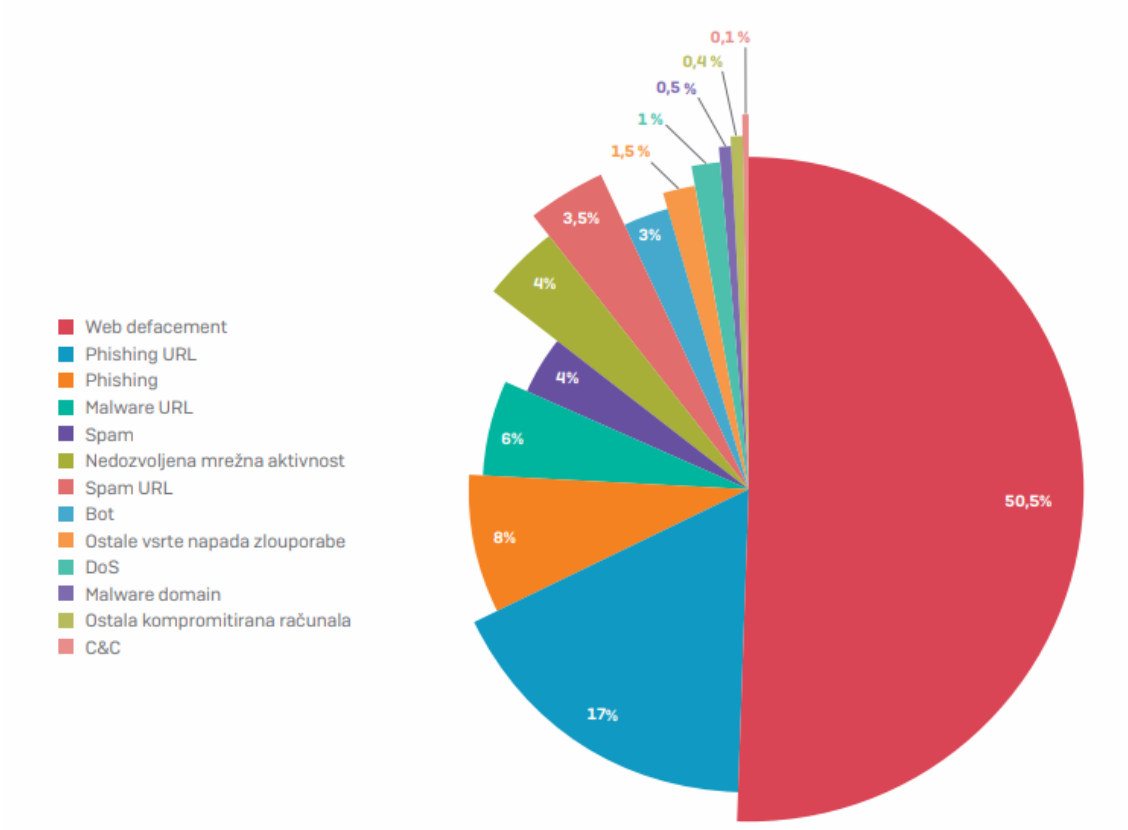
3.2. CERT

U Hrvatskoj, međutim, i danas djeluje Nacionalni CERT (eng. *Croatian National Computer Emergency Response Team*), osnovan 2007. godine koji, između ostalog, od 2015. objavljuje izvještaje za svaku tekuću godinu. Što se tiče područja djelovanja, za sebe kažu da im je „osnovna zadaća obrada incidenata na internetu odnosno očuvanje informacijske sigurnosti u Republici Hrvatskoj.“[28] Način na koji su incidenti obrađeni sličan je izvješćima CSI-a, jedino što se CERT, za razliku od njih, ne bavi toliko reakcijama korisnika, koliko tipovima incidenata općenito. (Slike 3. i 4.)

TIP INCIDENTA	BROJ	TREND
Web defacement	370	▲
Phishing URL	127	▼
Phishing	59	▲
Malware URL	42	▼
Spam	29	▲
Nedozvoljena mrežna aktivnost	28	▲
Spam URL	26	▲
Bot	20	▲
Ostale vrste napada i zlouporabe	12	▲
DoS	10	▼
Malware domain	4	▲
Ostala kompromitirana računala	3	▼
C&C	2	–
UKUPNO	732	▲

Slika 3. Prikaz incidenata po tipu u 2017. godini.[29]

[28]Nacionalni CERT. Godišnji izvještaj Nacionalnog CERT-a za 2017. godinu, 2017. Str. 2. Dostupnona: https://www.cert.hr/wp-content/uploads/2018/03/CERT.hr_godisnji_izvjestaj_2017.pdf
[29]Nacionalni CERT. GodišnjiizvještajNacionalnog CERT-a za 2017.godinu, 2017.Dostupnona: https://www.cert.hr/wp-content/uploads/2018/03/CERT.hr_godisnji_izvjestaj_2017.pdf



Slika 4. Raspodjela incidenata po tipu u 2017. godini.[30]

Treba uzeti u obzir, naravno, da su ovo samo incidenti koji su prijavljeni, ali daleko najzastupljeniji incident je tzv. *web defacement*, odnosno izmjena stranica na mreži. Na drugom i trećem mjestu je tzv. *phishing*, o kojem je već bilo govora, a sve zajedno spada u skupinu kompromitiranja internetskih stranica, čiji je cilj krađa osobnih podataka. Dakle, zlouporabe koje se temelje na pokušajima krađe osobnih podataka pokrivaju više od tri četvrtine svih računalnih incidenata.

Osim objavljivanjem godišnjih izvještaja, CERT se trudi na mnoge načine osvijestiti korisnike o opasnostima koje se kriju na Internetu. Na njihovoj internetskoj stranici[31] postoji tzv. „baza znanja“ gdje korisnici mogu naći razne brošure koje daju savjete za sigurnije korištenje Interneta. Isto tako, moguće je direktno sa stranice preuzeti dokumente i prezentacije koji se bave

[30]Nacionalni CERT. GodišnjiizvještajNacionalnog CERT-a za 2017.godinu, 2017.Dostupnona: https://www.cert.hr/wp-content/uploads/2018/03/CERT.hr_godisnji_izvjestaj_2017.pdf
[31]CERT.hr (2018) URL: https://www.cert.hr/ (25.8.2018.)

aktualnim problemima i mjerama zaštite. Svakodnevno se na njihovoj stranici objavljuju i razne novosti vezane uz događaje na mreži, kao i preporuke vezane uz sigurnosne nedostatke pojedinih programa.

Svake godine predstavljaju i brojne projekte na kojima u tom trenutku rade. U zadnjem izvještaju predstavili su najnoviji projekt pod nazivom GrowCERT. Projekt su opisali ovako: „Provedbom projekta doprinosi se jačanju nacionalnih kapaciteta za prikupljanje, analizu i razmjenu informacija o kibernetičkim incidentima i prijetnjama kibernetičkoj sigurnosti korištenjem novorazvijene platforme za prikupljanje podataka o sigurnosnim incidentima na nacionalnoj i europskoj razini. Ovim projektom želi se podići svijest o kibernetičkim prijetnjama te adekvatnim odgovorima na iste.“[32]Dakle, ovaj dvogodišnji projekt usmjeren je, kao što mu i samo ime kaže, na razvijanje CERT-a kako bi korisnicima omogućio što bolju platformu za suočavanje s računalnim kriminalitetom i kako bi učvrstio sigurnost na mreži. Na ovom projektu, ali i na brojnim drugim projektima, surađuju sa zemljama iz cijeloga svijeta, kao i s poznatim međunarodnim organizacijama, kao što su Europska Unija, NATO i Europska komisija.

4 Zaštita od zlouporabe podataka

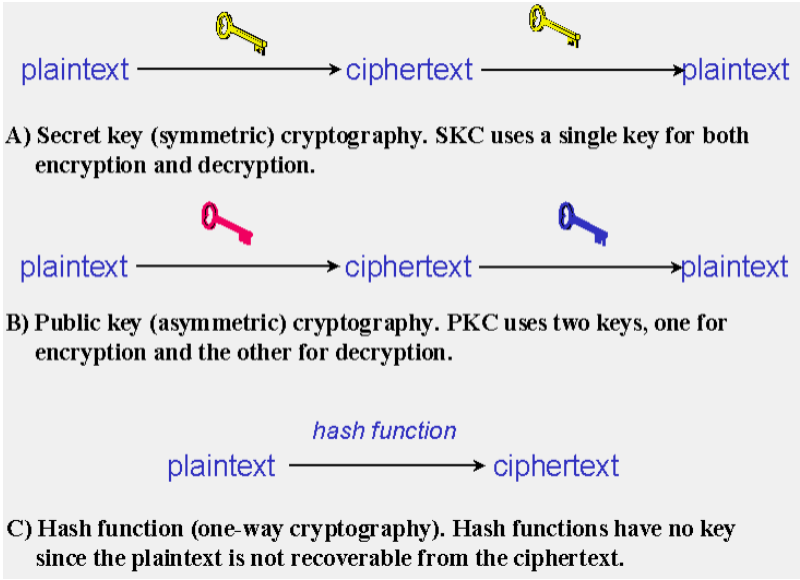
M. Boban u svom radu spominje neke od metoda i sredstava zaštite na mreži, kao što su fizička zaštita, provjera pristupa, kriptografija, digitalni certifikat, digitalni potpis, steganografija, vatreni zid, sigurnosne kopije, zaštita od virusa i nadzor i analiza rada.[33]

Fizička zaštita, kao što joj i samo ime kaže, odnosi se na mjere zaštite koje možemo učiniti u materijalnom svijetu, kao što je zaštita uređaja od krađe, neovlaštenog pristupa i slično. Najčešća zaštita od neovlaštenog pristupa, ali ne u fizičkom smislu, je provjera pristupa. Većinom se upotrebljavaju lozinke, ali razvoj tehnologije omogućio je i preciznije mjere zaštite, koristeći karakteristike koje su specifične samo za jednu osobu, kao što je otisak prsta ili zjenice, odnosno biometrijska identifikacija. Indija se nedavno upustila u pothvat prikupljanjabiometrijskih podataka svih svojih stanovnika (cca. 1 milijarde) kako bi pomoću njih

[32] Nacionalni CERT. Godišnji izvještaj Nacionalnog CERT-a za 2017. godinu, 2017. Str. 12.Dostupnona: https://www.cert.hr/wp-content/uploads/2018/03/CERT.hr_godisnji_izvjestaj_2017.pdf
[33]Boban, Sigurnost i zaštita osobnih podataka, n. dj. Str. 86-88.

stvorila jedinstvene osobne iskaznice pod nazivom „Aadhaar“.[34] Svakoj osobi dodijelio bi se jedinstveni 12-znamenkasti broj kojim bi obavljali sve financijske transakcije. No, mnogo ljudi zabrinuto je u vezi sigurnosti takvog sustava, kao i nedovoljnih mjera zaštite privatnosti i osobnih podataka. Također, pojavila se sumnja da je ovaj sustav omogućio i olakšao nadziranje stanovnika, kao u jednoj regiji Kine, Xinjiang, gdje je razina kontrole koju država ima nad stanovnicima neizmjerno velika (koriste sistem prepoznavanja lica, nadzorne kamere i biometrijske podatke).[35]

Kriptografija se odnosi na zaštitu određenog sadržaja izmijenjujući ga tako da izvoran neizmjenjeni tekst ne može vidjeti nitko tko ne posjeduje šifru potrebnu za dešifriranje sadržaja. Postoje tri različite metode kriptografije. (Slika 5.)



Slika 5. Metode kriptografije.[36]

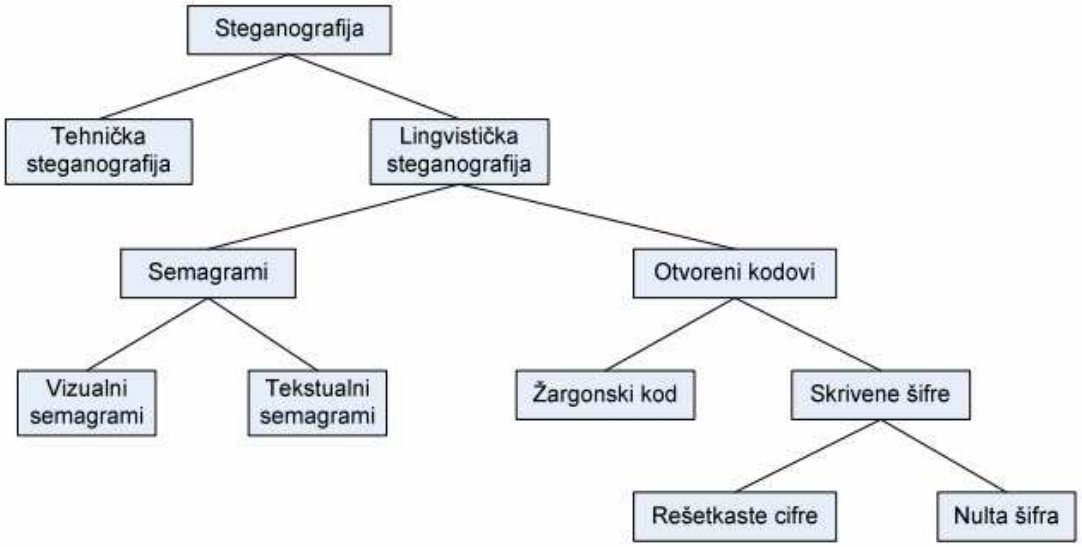
Kao što je vidljivo na slici, prva metoda je šifriranje tajnim, odnosno simetričnim ključem, kada se isti ključ koristi i za šifriranje i za dešifriranje. Druga mogućnost je šifriranje

[34] India Aadhaar ID cards: Collecting biometric data from 1bn people. 23.6.2017. URL: https://www.bbc.co.uk/news/world-asia-40371523 (25.8.2018.)
[35] Viewpoint: The pitfalls of India's biometric ID scheme. 23.4.2018. URL: https://www.bbc.co.uk/news/world-asia-india-43619944 (25.8.2018.)
[36] Kessler, Gary C. An Overview of Cryptography. 11.8.2018. URL: https://www.garykessler.net/library/crypto.html (25.8.2018.)

javnim, odnosno nesimetričnim ključem, gdje postoje dva ključa, od kojih jedan služi za šifriranje, a drugi za dešifriranje. I naposljetku, jednosmjerno šifriranje, za koje nije potreban ključ zato što tekst nije namijenjen dešifriranju, te se ne može doći do izvornog sadržaja.

Digitalni certifikat i digitalni potpis koriste se u radu s dokumentima preko mreže. „Digitalni certifikat je isprava u digitalnom obliku kojom se potvrđuje identitet neke pravne ili fizičke osobe. (...) Digitalni potpis koristi se za provjeru kada je digitalni dokument kreiran, odnosno zadnji puta promijenjen, što je važno za utvrđivanje vjerodostojnosti dokumenata.“[37]U Hrvatskoj se izdavanjem digitalnih certifikata bavi Fina.

Steganografija se bavi skrivanjem informacija unutar drugih dokumenata ili poruka na mreži, kako bi se osigurala tajnost razmjene podataka između pošiljatelja i primatelja. Postoje različite tehnike i načini skrivanja informacija. (Slika 6.)



Slika 6. Pregled steganografskih tehnika.[38]

Tehnička steganografija odnosi se na znanstvene metode, npr. nevidljiva tinta, dok se lingvistička steganografija odnosi na skrivanje poruke unutar određenog nositelja koji izgleda

[37]Boban, Sigurnost i zaštita osobnih podataka, n. dj. Str. 87.
[38]CARNet.Steganografija, 2006.Dostupnona: https://www.cis.hr/www.edicija/LinkedDocuments/CCERT-PUBDOC-2006-04-154.pdf

kao nešto što nema nikakve veze sa skrivenom porukom. Semagrami skrivaju informacije uz pomoć simbola i znakova, npr. poseban razmještaj objekata na internetskoj stranici (vizualni semagram) ili promjena veličine ili tipa fonta (tekstualni semagram). Pod otvorene kodove spadaju poruke u kojima nositelj predstavlja javnu komunikaciju, odnosno komunikaciju koja nije skrivena. Žargonski kod je terminologija poznata samo određenoj skupini ljudi, dok je kod skrivenih šifri moguće doći do skrivene poruke jedino ako nam je poznata metoda kojom je poruka sakrivena. Dijele se na rešetkaste (skrivena poruka se otkriva pomoću predloška) i nulte šifre (postoji određen skup pravila za pronalazak skrivene poruke).[39]

Vatreni zid (eng. *firewall*) potreban je za sigurniji pristup Internetu, a kako bi se zaštitili i od računalnih virusa, najbolje je upotrebljavati neki antivirusni program. Sigurnosne kopije (eng. *backup*) koriste se za zaštitu podataka u slučaju mogućeg kvara na računalu. Nadzor i analiza rada potrebni su kako bi se uočile potencijalne slabosti ili jesu li potrebne nove mjere sigurnosti.

4.1. ISO norme

„U cilju sustavne zaštite informacijskih sustava definirane su različite norme kojima se, na različite načine, nastoje obuhvatiti kompletni sustavi za upravljanje sigurnošću ili neki njegovi aspekti.“[40] Međunarodna organizacija za standardizaciju (eng. *International Organization for Standardization – ISO*) bavi se objavljivanjem normi na međunarodnoj razini. Hrvatski zavod za norme usvojio je dvije međunarodne norme informacijske sigurnosti: HRN ISO/IEC 27001 i HRN ISO/IEC 17799. Hrvatske norme nose nazive „Sustavi upravljanja informacijskom sigurnošću – Zahtjevi“ i „Kodeks postupaka za upravljanje informacijskom sigurnošću“. O njihovoj važnosti u svome radu govori J. Bogati. „Kao rezultat implementiranja normi informacijske sigurnosti dobiva se jasno definiran okvir nadležnosti, odgovornosti i ovlasti unutar informacijskog sustava. One su, kao rezultat sigurnosnih zahtjeva, prevedene u procedure unutar sigurnosnih pravilnika i ostalih dokumenata.“[41]

[39] CARNet. Steganografija, 2006.Dostupnona: https://www.cis.hr/www.edicija/LinkedDocuments/CCERT-PUBDOC-2006-04-154.pdf

[40] Boban, Sigurnost i zaštita osobnih podataka, n. dj. Str. 154.

[41] Bogati, Javor. Norme informacijske sigurnosti ISO/IEC 27K. // Praktični menadžment : stručni časopis za teoriju i praksu menadžmenta. 2, 2(2011), str. 116.

Prije govora o implementiraju samih normi, potrebno je spomenuti model PDCA (eng. *Plan-Do-Check-Act*) ciklusa pomoću kojeg je opisan način upravljanja informacijskom sigurnošću. (Slika 7.)

Slika 7. Shema PDCA ciklusa.[42]

Sustav upravljanja informacijskom sigurnošću (eng. *Information Security Management System – ISMS*) ključan je dio tog procesa. Faze PDCA ciklusa, kako ih je J. Bogati opisao, su: „PLAN: uspostava sustava za upravljanje informacijskom sigurnošću; DO: upravljanje sustavom informacijske sigurnosti; CHECK: nadzor i ispitivanje sustava informacijske sigurnosti; ACT: poboljšanje sustava informacijske sigurnosti“[43] Sve faze se međusobno nadopunjavaju i potrebno ih je cijelo vrijeme provoditi kako bi se osigurala što efikasnija informacijska sigurnost.

Osim toga, postoje upute za ispravnu implementaciju ISO normi, koja se, prema J. Bogati, sastoji od osam koraka: započinjanje projekta, definiranje ISMS-a, procjena rizika, upravljanje rizikom, obuka i osvješćivanje, priprema za reviziju, revizija i neprekidno osvješćivanje.[44] Dakle, potrebno je najprije upoznati se sa sustavom upravljanja informacijskom

[42]Bogati, Normeinformacijskesigurnosti ISO/IEC 27K, n. dj.
[43]Bogati, Norme informacijske sigurnosti ISO/IEC 27K, n. dj. Str. 114.
[44] Bogati, Norme informacijske sigurnosti ISO/IEC 27K, n. dj. Str. 115-116.

sigurnošću (ISMS-om), a potom procijeniti sve potencijalne opasnosti koje bi mogle ugroziti informacijsku sigurnost kako bi se mogli poduzeti koraci ka rješavanju problema. Naravno, treba se pobrinuti i za to da su svi koji su uključeni u ovaj postupak adekvatno pripremljeni. No, čak i nakon revizije, potrebno je redovito provjeravati i obnavljati sustav, ako za to bude potrebe.

5Prvi incidenti

Od samih početaka Interneta do danas, korisnici su se susretali s raznim kontroverzama i skandalima vezanim uz zlouporabu podataka. Facebook je danas najaktualniji, ali s obzirom na to da nije postojao u periodu kada se Internet počeo razvijati, dobro je osvrnuti se i na probleme koji su se javljali tada. Laura J. Gurak u svojoj knjizi „Persuasion and Privacy in Cyberspace“ iz 1997. godine analizira neke od najranijih incidenata vezanih uz privatnost na mreži. Jedan od njih vezan je uz Lotus MarketPlace.[45]

LotusMarketPlace bila je baza podataka dizajnirana kako bi olakšala poslovnu komunikaciju, odnosno kako bi manjim poduzećima olakšala pronalaženje potencijalnih klijenata. Projekt je bio podijeljen na dva dijela, prvi dio sadržavao je podatke o tvrtkama, a drugi dio, daleko kontroverzniji, raznorazne osobne podatke, kao što su ime i prezime, adresa, godine, spol, bračni status, godišnji prihodi, pa čak i kupovne navike ljudi. Projekt je bio otkazan čim se pojavio na tržištuzbog brojnih tužbi i prosvjeda na račun povrede privatnosti.

Iako im je cilj bio olakšati manjim poduzećima poslovanje, i iako činjenica da su u prvom dijelu svog projekta koristili podatke o drugim tvrtkama nije bila kontroverzna, svejedno su povrijedili privatnost mnogima iznoseći njihove osobne podatke bez njihova dopuštenja. Naravno, tvrdili su da tim podacima mogu pristupiti samo provjerena i autorizirana poduzeća koja će plaćati za pristup informacijama, ali također je postojala i opasnost da će netko neautoriziran pristupiti bazi podataka i domoći se tuđih osobnih podataka. Baze podataka su trebale biti objavljivane na CD-ROM-ovima, pa čak i ako se uzme u obzir činjenica da su omogućili opciju da se osobe čiji se podaci nalaze u bazi ako žele jave i zatraže da se ti podaci

[45] Gurak, Laura J. Persuasion and Privacy in Cyberspace. New Haven, London : Yale University Press, 1997.

uklone, njihovi osobni podaci bili bi uklonjeni samo iz novih izdanja, dok bi ostali u rukama onih koji su kupili starije verzije baza podataka.

6 Facebook

Facebook je postao sinonim za društvenu mrežu. Od samoga početka djelovanja do danas doživio je razvoj nezamislivih razmjera. Koriste ga milijuni, ako ne i milijarde ljudi svakoga dana. Iako je na početku bio zamišljen kao mreža za povezivanje studenata Harvarda, danas služi kao mreža za povezivanje cijeloga svijeta. Stoga je na primjeru Facebooka najbolje oslikati probleme vezane uz privatnost na Internetu, s obzirom na to da je doseg Facebooka toliko velik da se može usporediti s dosegom samoga Interneta.

Kao što je već navedeno, Facebook je stvoren 2004. godine s namjerom da omogući lakše povezivanje studenata Harvarda, da bi potom 2006. postao dostupan svima. Pri stvaranju korisničkog računa na Facebooku, korisnici su davali određene informacije o sebi, koje su prvotno trebale biti vidljive samo ljudima na istoj „mreži“, npr. ljudima koji pohađaju isti fakultet. Kako se Facebook širio, tako je dodavao nove mreže, npr. regionalne, korporativne i sl. No, nakon što se opseg korisnika proširio na cijeli svijet, koncept „mreža“ je izgubio svoju svrhu, pa su tako korisnici dobili priliku da sami odluče kome mogu omogućiti pristup svojim korisničkim profilima (nikome, svima, prijateljima, prijateljima prijatelja i sl.). Problemi su se počeli javljati kada je Facebook postao platforma na koju su druge korporacije mogle postaviti svoje aplikacije i time skupljati podatke korisnika. Naravno, korisnici su prije pristupa tim aplikacijama trebali pristati na dijeljenje svojih podataka, ali nitko nije na to obraćao previše pažnje.[46]

Kao što je navela A. Bechmann, glavni razlog čestih narušavanja privatnosti na Facebooku, a i na ostalim društvenim mrežama, je to što, za razliku od života izvan mreže, gdje se ugovori potpisuju u četiri oka i generalno se shvaća na što se točno pristaje, ovdje se takve stvari obavljaju tako da korisniku iskoči prozorčić u kojemu on treba pritisnuti gumb i time dozvoliti pristup nekoj trećoj stranci kako bi se mogao što prije vratiti onome što je prije toga

[46]Boyd, Danah; Hargittai, Eszter. Facebook privacy settings: Who cares? // First Monday. 15, 8(2010)

radio.[47] Sam Internet oduvijek je predstavljao uštedu vremena, pa se i naša kultura pretvorila u kulturu uštede vremena. Uvijek negdje žurimo i cilj nam je u što manje vremena obaviti što više. Prestali smo obraćati pažnju na stvari na koje smo prije obraćali pažnju, pa tako više ne prepoznajemo situacije u kojima bi nam privatnost mogla biti ugrožena. No, nakon brojnih incidenata koji su došli na vidjelo, ljudi su ipak počeli obraćati pažnju na moguća narušavanja svoje privatnosti, i na pitanje smije li uopće Facebook davati informacije o svojim korisnicima trećim stranama, ako to nije točno specificirano i ako pristanak nije dobiven na neki drugi način osim kroz „prozorčiće" čije uvjeteprihvaćamo samo da ih se što prije riješimo.

Spominje se pojam „informiranog pristanka"[48]koji je ključ gotovo svakog problema vezanog uz privatnost koji se javio na Facebooku. Može li se pristanak korisnika na dijeljenje svojih osobnih podataka smatrati važećim ako nisu bili svjesni u kojoj su točno mjeri na to pristali? Internet je dodatno zakomplicirao pojam privatnosti, pretvarajući ga u svojevrsni paradoks, o čemu u svojoj knjizi govori H. Nissenbaum. Ona tvrdi da privatnost postoji isključivo kao paradoksalna veza između želje za samom privatnošću i potrebe za olakšavanjem i ubrzavanjem raznih procesa s kojima se suočavamo u životu. Također spominje paradoksalnu narav transparentnosti, tvrdeći da bi veća transparentnost na Internetu u vezi korištenja osobnih podataka korisnika uzrokovala pretrpanost informacijama, te ni tako ne bismo došli do riješenja.[49]Facebook od samih početaka pokušava pronaći način da u isto vrijeme zadovolji potrebe svojih korisnika, ali i svoje potrebe, kao i potrebe drugih korporacija koje traže načine da zarade korištenjem tuđih osobnih podataka. Zbog toga, a i zbog same naravi društvenih mreža kao takvih, Facebook je postao magnet za skandale vezane uz povrede privatnosti.

No, do sada najveći skandal vezan uz kontroverznost informiranog pristanka korisnika na dijeljenje svojih podataka dogodio se nedavno. Početkom 2018. godine Facebook i Cambridge Analytica našli su se u središtu velikog skandala vezanog za navodnu zlouporabu podataka Facebookovih korisnika.[50] Cambridge Analytica navodno je bila umiješana i u američke

[47]Bechmann, Anja. Non-Informed Consent Cultures: Privacy Policies and App Contracts on Facebook. // Journal of Media Business Studies. 11, 1(2014)
[48] Bechmann, Non-Informed Consent Cultures, n. dj.
[49]Nissenbaum, Helen. Privacy in Context: Technology, Policy, and the Integrity of Social Life. Stanford : Stanford University Press, 2010.
[50] Kleinman, Zoe. Cambridge Analytica: The story so far. 21.3.2018. URL: https://www.bbc.com/news/technology-43465968 (26.8.2018.)

predsjedničke izbore, te se navodi da je uz pomoć prikupljenih podataka potpomogla predsjedničkoj kampanji Donalda Trumpa. Do toga je došlo tako da su korisnici Facebooka 2014. godine imali priliku riješiti jedan od mnogih, naizgled bezazlenih psiholoških upitnika kakvi se često nude na Facebooku. Rješavajući upitnik, korisnici su nesvjesno omogućili prodaju svojih osobnih podataka, ali i osobnih podataka svih svojih prijatelja na Facebooku. Upitnik je riješilo 270.000 ljudi, a pribavljeni su osobni podaci njih 50 milijuna.Ljudi čiji su podaci proslijeđeni Cambridge Analytici većinom su bili državljani SAD-a, te su navodno iskorišteni za izradu psiholoških profila kojima je svrha bila poboljšati Trumpovu predsjedničku kampanju.

Osnivač Facebooka, Mark Zuckerberg, morao je odgovarati pred američkim Kongresom za povredu privatnosti i zlouporabu osobnih podataka korisnika do kojih je došlo u njegovoj nadležnosti. Facebookova službena izjava bila je da nisu bili svjesni tadašnjih događaja na svojoj platformi, ali da su aplikaciju putem koje su se skupljali podaci uklonili čim su saznali da su prava njihovih korisnika bila ugrožena. Jednako tako Cambridge Analytica tvrdi da nisu koristili ničije podatke, te da su ih obrisali čim im je Facebook tako naredio. No, u vezi toga i dalje postoje određene sumnje.

Nakon incidenta s Cambridge Analyticom, Facebook se našao u novim problemima nakon što se otkrilo da su određene tvrtke i dalje imale pristup osobnim podacima korisnika.[51] Naime, iako je to službeno bilo zabranjeno, nekim tvrtkama produžen je rok za prestanak prikupljanja osobnih podataka. Na listi ih je bilo navedeno 60, između ostalog Nike, Nissan i Spotify. Također, pristup podacima imale su i određene hardverske i softverske tvrtke, navodno kako bi mogle napraviti vlastite verzije Facebookovog sučelja. Na toj listi bili su HTC, Kodak, LG, Warner Bros i drugi, ali tim tvrtkama više nije omogućen pristup podacima korisnika. S druge strane, Facebook je izjavio da 14 tvrtki i dalje ima dopušten pristup podacima, neke od njih Nokia, Vodafone i Yahoo. Također su dodali da su njihovi analitičari utvrdili da nije bilo nikakvih povreda ili zlouporaba podataka od strane navedenih tvrtki s kojima imaju sporazum.

[51] Facebook reveals its data-sharing VIPs. 2.7.2018. URL: https://www.bbc.co.uk/news/technology-44682364 (26.8.2018.)

7GDPR

Opća odredba o zaštiti osobnih podataka (*eng. General Data Protection Regulation – GDPR*) stupila je na snagu 25. svibnja 2018. godine. Donio ju je Europski parlament, a pod njenu nadležnost spadaju sve tvrtke koje posluju na teritoriju EU, ali i tvrtke koje raspolažu podacima europskih građana, neovisno o njihovoj lokaciji. Kazna za nepoštivanje odredbe je do 4% ukupnog godišnjeg prometa na svjetskoj razini ili do 20 milijuna eura, ovisno o tome koji je iznos veći. Ova odredba razlog je brojnih promjena u politikama privatnosti podataka s kojima su se korisnici mogli susresti ove godine. Odredila je što sve spada pod osobne podatke i navela da korisnici moraju eksplicitno pristati na bilo kakvo dijeljenje osobnih podataka, dok se sve ostalo smatra povredom njihove privatnosti.[52]

Ova odredba dobrodošla je direktiva u svijetu tehnologije, naročito neposredno nakon svih afera i skandala. No, čim je stupila na snagu, došlo je do novih sukoba s internetskim divovima kao što su Facebook i Google.[53] Naime, optuženi su za to da nisu korisnici dali izbora što se tiče ciljanog oglašavanja koje se odvija na njihovim platformama.

Ne možemo znati hoće li se problemi vezani uz zaštitu podataka na mreži ikada razriješiti, ali barem se poduzimaju određeni koraci prema sigurnijem korištenju Interneta.

[52]Garg, Radhika. Open data privacy and security policy issues and its influence on embracing the Internet of Things. // First Monday. 23, 5(2018)
[53]Foxx, Chris. Google and Facebook accused of breaking GDPR laws. 25.5.2018. URL: https://www.bbc.com/news/technology-44252327 (26.8.2018.)

Zaključak

U današnjem svijetu nemoguće je biti dio normalne svakodnevice bez pristupa Internetu. Ne možemo znati je li se Internet razvio onako kako su njegovi tvorci očekivali, ali u svakom slučaju razvoj Interneta doživio je ogromne razmjere. I naravno, to je sa sobom donijelo određene opasnosti. Svaki put kada stupimo na mrežu, izloženi smo utjecajima sa svih strana. Naši osobni podaci mogu nekome pomoći da se obogati, i to na više načina. Netko bi mogao naše osobne podatke iskoristiti za ciljano oglašavanje i bolji marketing svog proizvoda. Netko bi ih mogao iskoristiti kako bi nam ukrao novce s bankovnog računa. U oba slučaja došlo je do povrede naše privatnosti, našeg fundamentalnog ljudskog prava.

Ono što nam je činiti je povećati svijest o mogućim zlouporabama podataka. Internet služi kao sredstvo, odnosno alat za krađu naših osobnih podataka, ali isto tako može služiti i kao sredstvo za zaštitu naših osobnih podataka. Postoji mnogo organizacija koje se na Internetu angažiraju kako bi suzbile računalni kriminalitet i potiču korisnike da im sa svojim iskustvima pomognu u tome. Isto tako, s razvojem Interneta kao medija, glas svakoga pojedinca može se čuti. Vrijednost informacije neizmjerno je velika, pa zašto ne bismo to iskoristili u svoju korist? Suočavanje Facebooka s optužbama za zlouporabu podataka možda je potaknulo Opću odredbu o zaštiti podataka da stupi na snagu. Lotus MarketPlace morao je otkazati projekt zato što su se ljudi pobunili zbog neovlaštenog korištenja njihovih osobnih podataka.

Internet nam je možda izvor brojnih sigurnosnih problema, ali je ujedno i rješenje.

Literatura

1. Abad, Christopher. The economy of phishing: A survey of the operations of the phishing market. // First Monday. 10, 9(2005)
2. Bechmann, Anja. Non-Informed Consent Cultures: Privacy Policies and App Contracts on Facebook. // Journal of Media Business Studies. 11, 1(2014)
3. Boban, Marija. Sigurnost i zaštita osobnih podataka - pravni i kulturološki aspekti : doktorska disertacija. Zagreb : Filozofski fakultet u Zagrebu : Odsjek za informacijske znanosti, 2012.
4. Bogati, Javor. Norme informacijske sigurnosti ISO/IEC 27K. // Praktični menadžment : stručni časopis za teoriju i praksu menadžmenta. 2, 2(2011)
5. Boyd, Danah; Hargittai, Eszter. Facebook privacy settings: Who cares? // First Monday. 15, 8(2010)
6. Branford, Becky. Information warfare: Is Russia really interfering in European states? 31.3.2017. URL: https://www.bbc.com/news/world-europe-39401637 (24.8.2018.)
7. CARNet. Steganografija, 2006. Dostupno na: https://www.cis.hr/www.edicija/LinkedDocuments/CCERT-PUBDOC-2006-04-154.pdf
8. CERT.hr (2018) URL: https://www.cert.hr/ (25.8.2018.)
9. Claessens, Joris; Preneel, Bart; Vandewalle, Joos. A Tangled World Wide Web of Security Issues. // First Monday. 7, 3(2002)
10. Computer Security Institute. 2010/2011 Computer Crime and Security Survey, 2011. Dostupno na: https://cours.etsmtl.ca/gti619/documents/divers/CSIsurvey2010.pdf
11. Facebook reveals its data-sharing VIPs. 2.7.2018. URL: https://www.bbc.co.uk/news/technology-44682364 (26.8.2018.)
12. Foxx, Chris. Google and Facebook accused of breaking GDPR laws. 25.5.2018. URL: https://www.bbc.com/news/technology-44252327 (26.8.2018.)
13. Garg, Radhika. Open data privacy and security policy issues and its influence on embracing the Internet of Things. // First Monday. 23, 5(2018)
14. Gurak, Laura J. Persuasion and Privacy in Cyberspace. New Haven, London : Yale University Press, 1997.

15. Haker. // Hrvatski jezični portal (2018), URL: http://hjp.znanje.hr/index.php?show=search_by_id&id=fV5iWRE%3D&keyword=haker (23.8.2018.)

16. India Aadhaar ID cards: Collecting biometric data from 1bn people. 23.6.2017. URL: https://www.bbc.co.uk/news/world-asia-40371523 (25.8.2018.)

17. Johnson, David R.; Post, David. Law and Borders – The Rise of Law in Cyberspace. // First Monday. 1, 1(1996)

18. Julian Assange: Campaigner or attention-seeker? 30.7.2018. URL: https://www.bbc.com/news/world-11047811 (23.8.2018.)

19. Kessler, Gary C. An Overview of Cryptography. 11.8.2018. URL: https://www.garykessler.net/library/crypto.html (25.8.2018.)

20. Kleinman, Zoe. Cambridge Analytica: The story so far. 21.3.2018. URL: https://www.bbc.com/news/technology-43465968 (23.8.2018.)

21. Miller, Michael. Apsolutna zaštita PC-ja i privatnosti. Čačak : Kompjuter biblioteka, 2003.

22. Nacionalni CERT. Godišnji izvještaj Nacionalnog CERT-a za 2017. godinu, 2017. Dostupno na: https://www.cert.hr/wp-content/uploads/2018/03/CERT.hr_godisnji_izvjestaj_2017.pdf

23. Nissenbaum, Helen. Privacy in Context: Technology, Policy, and the Integrity of Social Life. Stanford : Stanford University Press, 2010.

24. Tiku, Nitasha. Why Your Inbox Is Crammed Full of Privacy Policies. 24.5.2018. URL: https://www.wired.com/story/how-a-new-era-of-privacy-took-over-your-email-inbox/ (23.8.2018.)

25. Viewpoint: The pitfalls of India's biometric ID scheme. 23.4.2018. URL: https://www.bbc.co.uk/news/world-asia-india-43619944 (25.8.2018.)

26. Wright, Nicola. Death and the Internet: The implications of the digital afterlife. // First Monday. 19, 6(2014)

27. Zakon o zaštiti osobnih podataka. Zagreb : Narodne novine br. 103/2003.